

AMENDMENTS TO THE CLAIMS

Claim 1 (Currently Amended) A key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a supplyable number, which is a number indicating a number of times the decryption key can be supplied to a terminal apparatus connected to the key delivery apparatus via a network, the key delivery apparatus comprising:

a receiving unit ~~operable~~ configured to receive, from the terminal apparatus, a supply request, which is a request for the decryption key;

a supply determining unit ~~operable~~ configured, ~~if the terminal apparatus is a legitimate supply target,~~ to determine whether the terminal apparatus is a terminal apparatus of a first-type that manages a content-usage period, and whether the terminal apparatus is a terminal apparatus of a second-type that does not manage the content-usage period; and

a key supply unit ~~operable~~ configured, ~~when~~ if the supplyable number indicates that the decryption key can be supplied, to supply, to the terminal apparatus, (i) the decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, ~~when~~ if the supply determining unit determines that the terminal apparatus is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal apparatus, ~~when~~ if the supply determining unit determines that the terminal apparatus is of the second-type, wherein

the supply request includes one of first information and second information, the first information indicating that the encrypted content is stored in the terminal apparatus, and the second information indicating that the encrypted content is stored on a portable recording medium inserted into the terminal apparatus.

the supply determining unit determines, based on the received supply request, whether the terminal apparatus records the encrypted content on the portable recording medium, and

the supply determining unit determines that the terminal apparatus is of the first-type, when the supply determining unit determines if that the terminal apparatus records the encrypted content, the decryption key, and the key usage period onto a the portable recording medium.

Claim 2 (Previously Presented) The key delivery apparatus of claim 1, wherein:

the network is a home network connected to an external network;

content is received from outside the home network; and

the key delivery apparatus determines whether each terminal apparatus connected to the home network is a legitimate supply target.

Claim 3 (Currently Amended) The key delivery apparatus of claim 1, further comprising:

a key-information storage unit operable configured to store the key-usage period subsequent to the key supply unit supplying the decryption key and the key-usage period to the terminal apparatus of the first-type;

a period determining unit operable configured to determine whether the key-usage period has expired; and

a time management unit operable configured to add “1” to the suppliable number when the period determining unit determines that the key-usage period has expired.

Claim 4 (Currently Amended) The key delivery apparatus of claim 3, further comprising:

a date-time storage unit ~~operable~~configured to store at least one of a first group and a second group, the first group including (i) date-time information indicating the key-usage period and a supply date-time of the decryption key, and (ii) identification information indicating the supply target to be the terminal apparatus of the first-type, and the second group including (i) date-time information indicating the supply date-time of the decryption key, and (ii) identification information indicating the supply target to be the terminal apparatus of the second-type;

a date-time determining unit ~~operable~~configured to determine whether a present date-time has reached the supply date-time; and

a date-time supply unit ~~operable~~configured, when the data time determining unit determines that the present date-time has reached the supply date-time, to supply the decryption key and the key-usage period to the terminal apparatus of the first-type or supply the decryption key to the terminal apparatus of the second-type, based on the identification information.

Claim 5 (Currently Amended) The key delivery apparatus of claim 4, further comprising:

a search requesting unit ~~operable~~configured to transmit, to the terminal apparatus of the first-type and the terminal apparatus of the second-type, search information identifying the decryption key; and

a proprietary information receiving unit ~~operable~~configured to receive information indicating whether the decryption key is stored by the terminal apparatus of the first-type or the terminal apparatus of the second-type.

Claim 6 (Currently Amended) The key delivery apparatus of claim 5, wherein:

the key delivery apparatus stores secret information, which is information to be used as a reference when determining whether the terminal apparatus is the legitimate supply target;

the supply determining unit includes an authentication subunit ~~operable~~configured to determine whether the terminal apparatus is storing the secret information; and

the supply determining unit determines that the terminal apparatus is the legitimate supply target when the supply determining unit determines that the terminal apparatus is storing the secret information.

Claim 7 (Currently Amended) The key delivery apparatus of claim 6, wherein:

the key supply unit includes a remaining number determining subunit ~~operable~~configured to determine whether the suppliable number is greater than a predetermined reference number; and

the key supply unit determines that the suppliable number indicates that the decryption key can be supplied when the key supply unit determines that the suppliable number is greater than the predetermined reference number.

Claim 8 (Currently Amended) The key delivery apparatus of claim 7, wherein:

the key supply unit further includes an encryption subunit ~~operable~~configured (i) to encrypt the decryption key and the key-usage period when the decryption key and the key-usage period are to be supplied to the terminal apparatus of the first-type, and (ii) to encrypt the

decryption key when the decryption key is to be supplied to the terminal apparatus of the second-type; and

the key supply unit, when the key supply unit determines that the suppliable number indicates that the decryption key can be supplied, supplies to the terminal apparatus, (i) the encrypted decryption key and the encrypted key-usage period when it is determined that the terminal apparatus is of the first-type, and (ii) the encrypted decryption key when it is determined that the terminal apparatus is of the second-type.

Claim 9 (Currently Amended) The key delivery apparatus of claim 8, further comprising:

a historical information storage unit operable/configured to store historical information indicating a connection date-time of the terminal apparatus of the first-type;

a connection determining unit operable/configured to determine, using the connection date-time, whether the terminal apparatus of the first-type was connected to the network within a predetermined connection period; and

a connection management unit operable/configured to add “1” to the suppliable number when it is determined that the terminal apparatus of the first-type was not connected to the network within the predetermined connection period.

Claim 10 (Currently Amended) The key delivery apparatus of claim 8, further comprising:

a frequency storage unit operable/configured to store a usage frequency of the decryption key by the terminal apparatus of the first-type;

a frequency determining unit ~~operable~~configured to determine whether the usage frequency has reached a predetermined reference frequency; and

a connection management unit ~~operable~~configured to add “1” to the supplyable number when it is determined that the usage frequency has reached the predetermined reference frequency.

Claims 11-16 (Cancelled)

Claim 17 (Currently Amended) A portable recording medium that receives a supply of a decryption key, for decrypting an encrypted content, from a key delivery apparatus that manages the decryption key, the portable recording medium comprising:

a key reception unit ~~operable~~configured to receive the decryption key and a key-usage period of the decryption key from the key delivery apparatus, when the key delivery apparatus determines that supplying the decryption key to the portable recording medium is possible;

a key-information storage unit ~~operable~~configured to store the decryption key and the key-usage period;

a proprietary determining unit ~~operable~~configured to receive, from the key delivery apparatus, search information identifying the decryption key, and ~~operable~~configured to determine whether the decryption key is stored on the portable recording medium based on the search information; and

a proprietary notifying unit ~~operable~~configured to transmit, to the key delivery apparatus, predetermined information indicating that the decryption key is stored on the portable recording

medium, the predetermined information indicating that the decryption key is stored on the portable recording medium and being transmitted when the proprietary determining unit determines that the decryption key is stored on the portable recording medium.

Claims 18-20 (Cancelled)

Claim 21 (Currently Amended) A key delivery system comprising:

a key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a suppliable number, which is a number indicating a number of times the decryption key can be supplied to a terminal apparatus connected to the key delivery apparatus via a network;

a first-type terminal apparatus that manages a content-usage period; and

a second-type terminal apparatus that does not manage the content-usage period,

wherein:

the key delivery apparatus includes:

a receiving unit operable configured to receive, from the terminal apparatus, a supply request, which is a request for the decryption key;

a supply determining unit operable configured, ~~if the terminal apparatus is a legitimate supply target,~~ to determine whether the terminal apparatus is a terminal apparatus of the first-type and whether the terminal apparatus is a terminal apparatus of the second-type; and

a key supply unit operable configured, ~~when,~~ if the suppliable number indicates that the decryption key can be supplied, to supply, to the terminal apparatus, (i) the decryption

key and a key-usage period which imposes a restriction on usage of content and is related to the decryption key, when, if the supply determining unit determines that the terminal apparatus is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal apparatus, when, if the supply determining unit determines that the terminal apparatus is the second-type;

the supply determining unit determines that the terminal apparatus is of the first-type when if the terminal apparatus records the encrypted content, the decryption key, and the key-usage period onto a portable recording medium;

the first-type terminal apparatus receives, from the key delivery apparatus, and stores ~~store~~ the decryption key and the key-usage period; and

the second-type terminal apparatus receives the decryption key from the key delivery apparatus, and uses ~~use~~ the decryption key for content usage, wherein

the supply request includes one of first information and second information, the first information indicating that the encrypted content is stored in the terminal apparatus, and the second information indicating that the encrypted content is stored on a portable recording medium inserted into the terminal apparatus,

the supply determining unit determines, based on the received supply request, whether the terminal apparatus records the encrypted content on the portable recording medium, and

the supply determining unit determines that the terminal apparatus is of the first-type when the supply determining unit determines that the terminal apparatus records the encrypted content on the portable recording medium.

Claim 22 (Currently Amended) A key supply method of using a key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a supplyable number, which is a number indicating a number of times the decryption key can be supplied to a terminal apparatus connected to the key delivery apparatus via a network, the key supply method comprising:

receiving, from the terminal apparatus, a supply request, which is a request for the decryption key, the supply request including one of first information and second information, the first information indicating that the encrypted content is stored in the terminal apparatus, and the second information indicating that the encrypted content is stored on a portable recording medium inserted into the terminal apparatus;

determining, based on the received supply request, whether the terminal apparatus records the encrypted content on the portable recording medium;

determining, ~~if the terminal apparatus is a legitimate supply target,~~ whether the terminal apparatus is a terminal apparatus of a first-type that manages a content-usage period and whether the terminal apparatus is a terminal apparatus of a second-type that does not manage the content-usage period; and

supplying, to the terminal apparatus, when if the supplyable number indicates that the decryption key can be supplied, (i) the decryption key and a key-usage period which imposes a restriction on usage of content and is related to the decryption key, when if the determining determines that the terminal apparatus is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal

apparatus, when, if the determining determines that the terminal apparatus is of the second-type, wherein

the determining of whether the terminal apparatus is a terminal apparatus of the first-type determines that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable recording medium.

Claim 23 (Cancelled)

Claim 24 (Currently Amended) A computer-readable recording medium storing a key supply computer program used by a key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a supplyable number, which is a number indicating a number of times the decryption key can be supplied to a terminal apparatus connected to a key delivery apparatus via a network, the key supply computer program causing the key delivery apparatus to execute a method comprising:

receiving, from the terminal apparatus, a supply request which is a request for the decryption key, the supply request including one of first information and second information, the first information indicating that the encrypted content is stored in the terminal apparatus, and the second information indicating that the encrypted content is stored on a portable recording medium inserted into the terminal apparatus;

determining, based on the received supply request, whether the terminal apparatus records the encrypted content on the portable recording medium;

determining, ~~if the terminal apparatus is a legitimate supply target,~~ whether the terminal apparatus is a terminal apparatus of a first-type that manages a content-usage period and whether the terminal apparatus is a terminal apparatus of a second-type that does not manage the content-usage period; and

supplying, to the terminal apparatus, ~~when,~~ if the supplyable number indicates that the decryption key can be supplied, (i) the decryption key and a key-usage period which imposes a restriction on usage of content and is related to the decryption key, ~~when,~~ if the determining determines that the terminal apparatus is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal apparatus, ~~when,~~ if the determining determines that the terminal apparatus is of the second-type, wherein

the determining of whether the terminal apparatus is a terminal apparatus of the first-type determines that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable recording medium.